



VPNs seguras con Mikrotik RouterOS

Objetivos de este microcurso

1. Dar a conocer los distintos tipos de VPNs que pueden implementarse para hacer posible el **teletrabajo**.
2. Presentar configuraciones simples para conectividad VPN segura utilizando **dispositivos de usuario final** como clientes y RouterOS como servidor.

Resumen de los temas

1. Qué son las VPNs y porque las utilizamos.
2. Configuración general de parámetros de conexión.
3. Configuración específica para cada protocolo*.
4. Aspectos de seguridad en el Firewall de RouterOS.

Qué son las VPNs y porque las utilizamos

Qué son las VPNs y porque las utilizamos

Una VPN (Virtual Private Network o Red Privada Virtual), es una tecnología de red que permite generar una **conexión segura** entre dos dispositivos a través de una red insegura como Internet.

- A. La conexión es simulada por **interfaces virtuales** que se generan en cada extremo, y que forman lo que llamamos túnel.
- B. La seguridad sería la **autenticación** que ocurre entre los dos extremos para “levantar” el túnel y el **cifrado** de datos aplicado a los datos que lo atraviesan.

Qué son las VPNs y porque las utilizamos

¿Por qué usamos las VPNs?

¡Por seguridad! Es una de las tecnologías más aceptadas para acceder de forma segura a una red remota. Acceder a redes remotas de forma directa o con técnicas de NAT no siempre es recomendado y puede traer consecuencias. De los ataques más comunes que se dieron en 2019, podemos mencionar:

- Ataques de Ransomware a servidores y PCs.
- Ataques al servicio WinBox de MikroTik RouterOS.
- Ataques a servicios VPN obsoletos o mal configurados.



Qué son las VPNs y porque las utilizamos

Tipos de VPN

Hay varios tipos, pero en este curso nos centraremos en las más populares que soporta RouterOS y que además sirven para conectarse desde **dispositivos de usuario final**.

- **L2TP+IPSec** (hay clientes para Windows, Mac y Android)
- **SSTP** (cliente en dispositivos Windows)
- **OpenVPN** (hay clientes para todos los sistemas operativos)

Nota: Los protocolos **L2TP** o **PPTP** se consideran inseguros!

Qué son las VPNs y porque las utilizamos

Los tipos de VPN mencionas se configuran desde el menú **PPP**.

Y aquí se presentan dos roles: **servidor** y **cliente/s**.

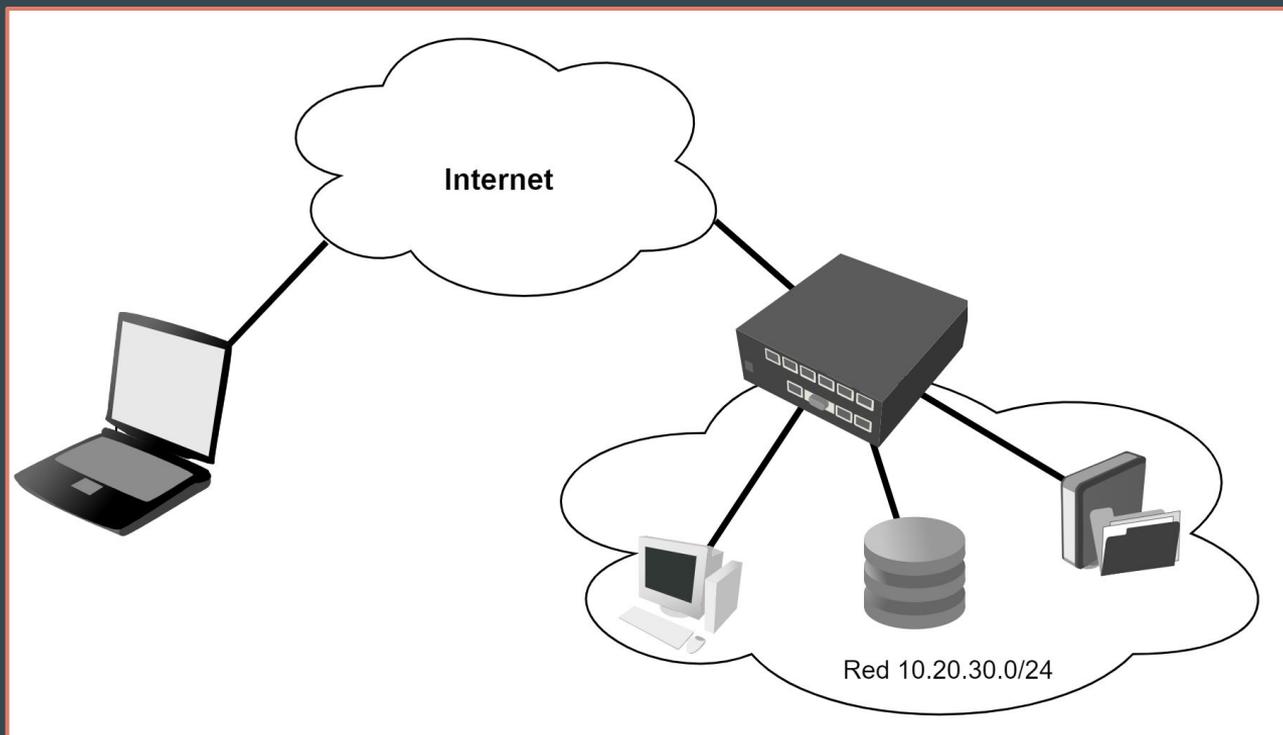
- El **servidor** queda a la espera de clientes, “escuchando” un puerto TCP o UDP en particular (dependiendo del tipo de VPN).
- El **cliente** es el que “marca” e intenta levantar el túnel contra un servidor (se requerirá un usuario y contraseña). En el escenario de este curso, esta configuración se realizaría desde una computadora o celular.

Configuración general de parámetros de conexión

Configuración general de parámetros de conexión

Escenario inicial:

- MikroTik con IP pública
- Red LAN 10.20.30.0/24
- Cliente remoto con IP pública o privada.
- En este escenario, muchos utilizan NAT (peligroso!).



Configuración general de parámetros de conexión

Dentro del menú PPP se harán las configuraciones para levantar un servidor, sin importar el protocolo elegido.

- **Configuración general**
 - Configuración de **Pool de IPs** (en [IP → Pool])
 - Configuración de **Perfiles** (en [PPP → Profiles])
 - Configuración de **Usuarios** (en [PPP → Secrets])
- **Configuración específica**
 - Configuración del **Protocolo** (PPTP, L2TP, SSTP, OVPN)



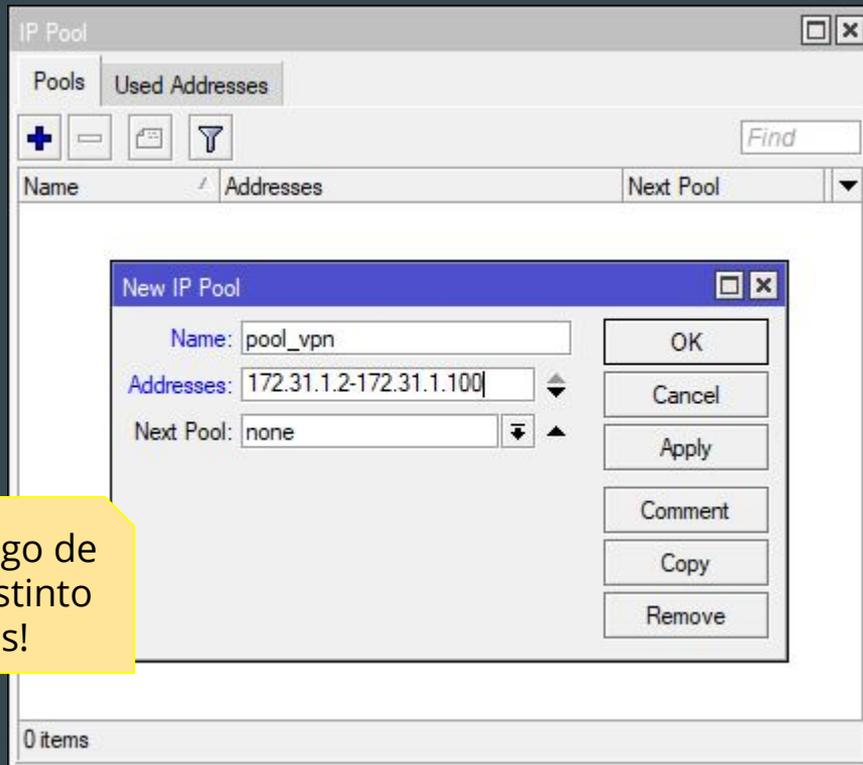
Configuración general de parámetros de conexión

El **Pool de IPs** se utiliza para configurar de forma automática, una dirección IP al extremo del túnel del **lado cliente**.

La dirección IP del extremo del túnel del **lado servidor** se podría obtener del Pool, pero hay otra forma que veremos más adelante.

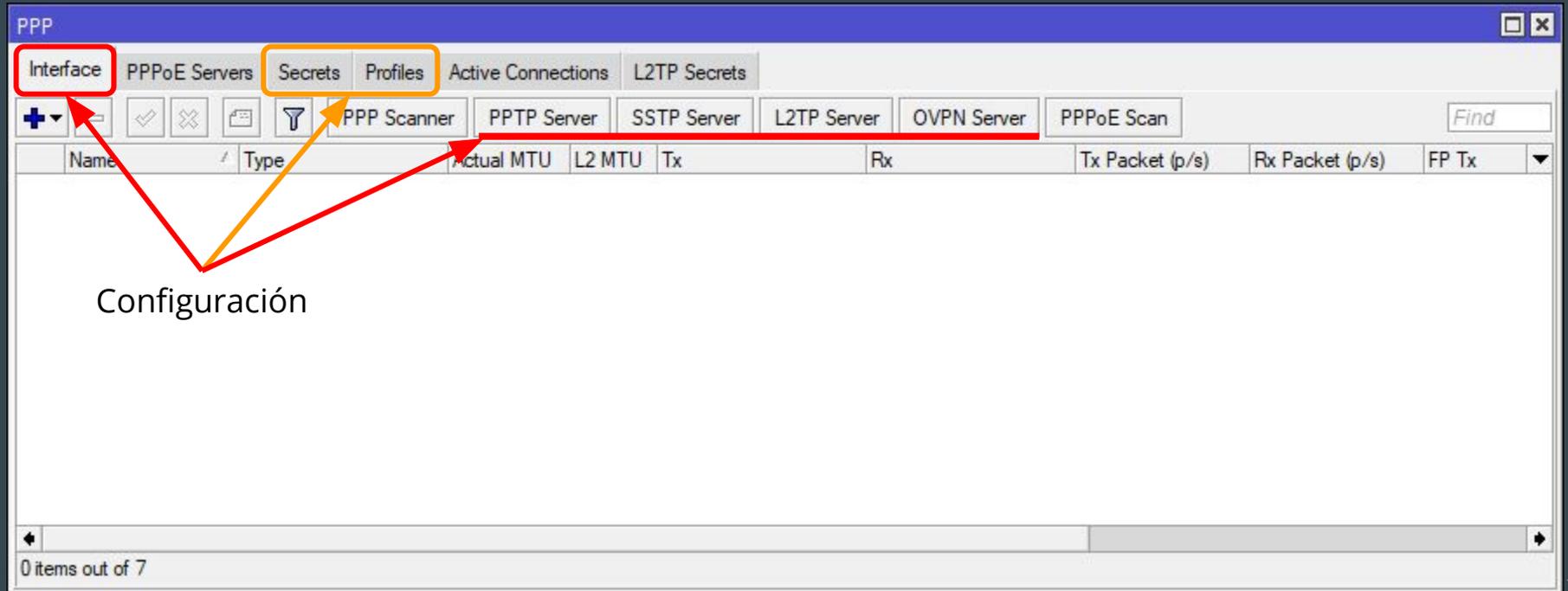
```
/ip pool add \  
name=pool_vpn \  
ranges=172.31.1.2-172.31.1.100
```

TIP: utilizar un rango de red específico y distinto de las redes locales!



Configuración general de parámetros de conexión

En el menú **PPP** se encuentra la mayoría de las configuraciones:



Configuración general de parámetros de conexión

Los perfiles definen parámetros aplicables a todos los usuarios (secrets) que lo utilicen. Se encuentra en [PPP → Profiles → +]

Local Address - Es la IP (o Pool) que se utilizará para el extremo local del túnel de cada cliente que use este perfil.

Remote Address - Es el Pool que se utilizará para darle una IP al extremo remoto del túnel de cada cliente que use este perfil.

```
/ppp profile add name=profile_vpn1 \  
local-address=172.31.1.1 remote-address=pool_vpn \  
dns-server=10.20.30.88 only-one=yes
```

New PPP Profile

General Protocols Limits Queue Scripts

Name: profile_vpn1

Local Address: 172.31.1.1

Remote Address: pool_vpn

Remote IPv6 Prefix Pool:

DHCPv6 PD Pool:

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server: 10.20.30.88

WINS Server:

- Change TCP MSS

no yes default

- Use UPnP

no yes default

OK

Cancel

Apply

Comment

Copy

Remove

Configuración general de parámetros de conexión

Las solapas **Protocols** y **Limits** tienen configuraciones adicionales.

Only One - Sólo se permite una conexión en simultáneo con el mismo usuario (secret).

PPP Profile <profile_vpn1>

General Protocols Limits Queue Scripts

OK Cancel Apply Comment Copy Remove

- Use IPv6
 no yes required default

- Use MPLS
 no yes required default

- Use Compression
 no yes default

Use Encryption
 no yes required default

PPP Profile <profile_vpn1>

General Protocols Limits Queue Scripts

OK Cancel Apply Comment Copy Remove

Session Timeout: []

Idle Timeout: []

Rate Limit (rx/tx): []

Only One
 no yes default

Configuración general de parámetros de conexión

Es la base de datos local de usuarios y se encuentra en [PPP → Secrets → +]

Permite definir en qué servicio PPP es aplicable la cuenta de usuario y el perfil que se va a utilizar.

```
/ppp secret add \  
name=usuario password=qV9AT8z7 \  
profile=profile_vpn1 service=any
```

New PPP Secret

Name: usuario

Password: qV9AT8z7

Service: any

Caller ID:

Profile: profile_vpn1

Local Address:

Remote Address:

Remote IPv6 Prefix:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Configuración general de parámetros de conexión

Pool de IPs para cada extremo remoto de los túneles que se conecten.

```
/ip pool add name=pool_vpn ranges=172.31.1.2-172.31.1.100
```

Perfil con configuraciones generales para todos los usuarios/túneles.

```
/ppp profile add name=profile_vpn1 \  
local-address=172.31.1.1 remote-address=pool_vpn \  
dns-server=10.20.30.88 only-one=yes
```

Usuario y contraseña para un usuario/túnel.

```
/ppp secret add name=usuario password=qV9AT8z7 \  
profile=profile_vpn1 service=any
```

Configuración específica para cada protocolo

L2TP+IPSec, SSTP y OpenVPN

Configuración específica para L2TP+IPSec

- L2TP utiliza **UDP 1701** para levantar un túnel entre cliente y servidor.
- IPSec se encarga del cifrado de datos, y para poder levantar, necesita los puertos **UDP 500**, **UDP 4500** y el protocolo **IPSec-ESP**.



Excelente compatibilidad.



Excelente cifrado.

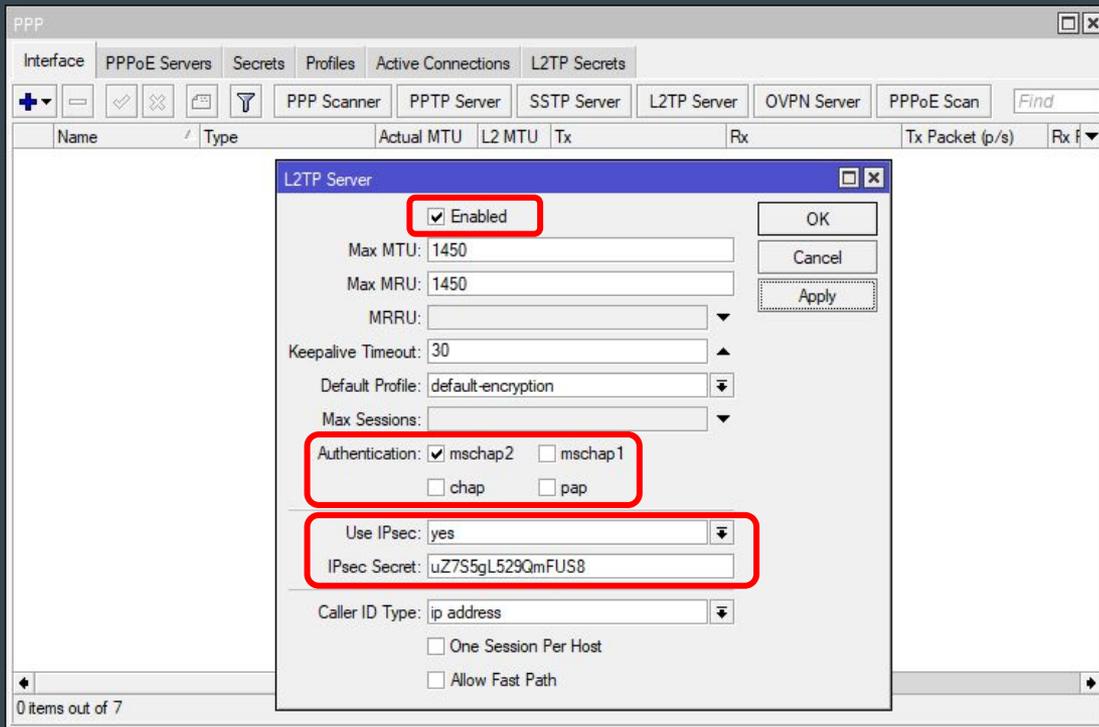


Algunos ISPs bloquean el protocolo IPSec-ESP o los puertos UDP 500 y/o 4500.

Configuración específica para L2TP+IPSec

1. Habilitarlo.
2. Configurar la autenticación a sólo mschap2.
3. Activar IPSec con una llave precompartida segura.

```
/interface l2tp-server server set \  
enabled=yes \  
authentication=mschap2 \  
use-ipsec=yes \  
ipsec-secret=uZ7S5gL529QmFUS8
```



Configuración específica para L2TP+IPSec

Ejemplo con
cliente Windows 10

The image shows a Windows 10 configuration window titled "Configuración" with the subtitle "Agregar una conexión VPN". The window contains several input fields and dropdown menus, with five specific fields highlighted by red rectangles:

- Proveedor de VPN:** A dropdown menu set to "Windows (integrado)".
- Nombre de conexión:** A text input field containing "VPN L2TP+IPSec".
- Nombre de servidor o dirección:** A text input field containing "vpn.dominio.com".
- Tipo de VPN:** A dropdown menu set to "L2TP/IPsec con clave previamente compartid".
- Clave previamente compartida:** A text input field filled with 12 dots.
- Tipo de información de inicio de sesión:** A dropdown menu set to "Nombre de usuario y contraseña".
- Nombre de usuario (opcional):** A text input field containing "usuario".
- Contraseña (opcional):** A text input field filled with 6 dots and a visibility icon.
- Recordar información de inicio de sesión:** A checked checkbox.
- Buttons:** "Guardar" and "Cancelar" buttons at the bottom right.

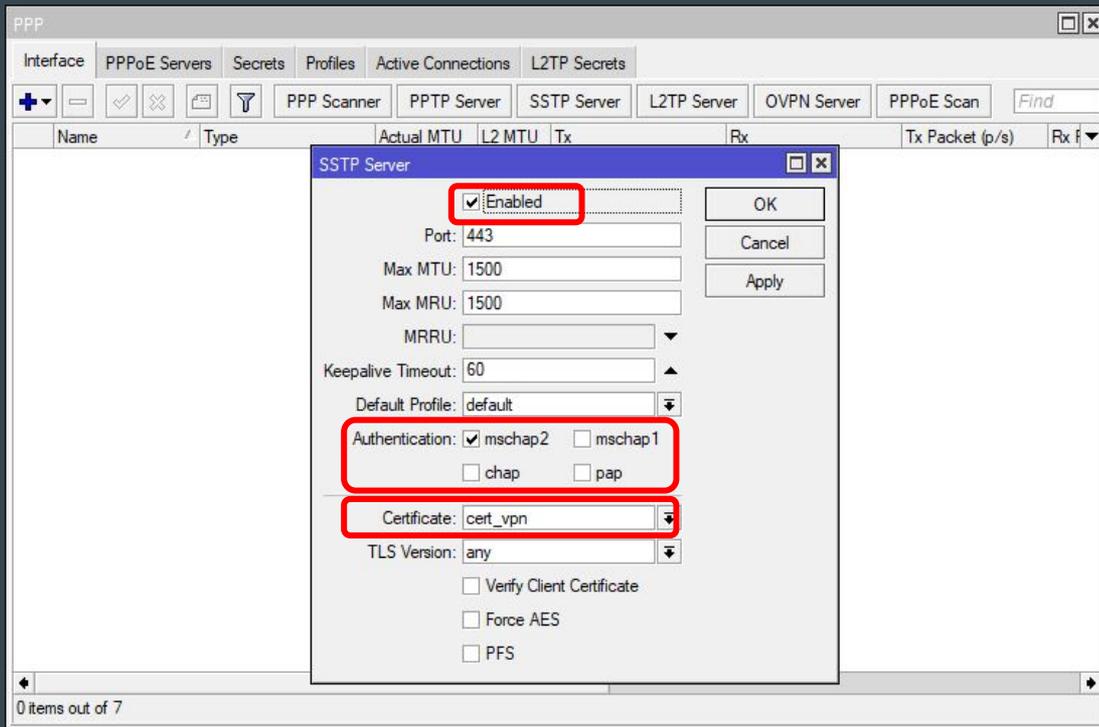
Configuración específica para SSTP

- SSTP utiliza **TCP 443** (aunque se puede cambiar) para levantar un túnel entre cliente y servidor, utilizando los mecanismos de TLS (HTTPs).
- 👍 Buena compatibilidad.
- 👍 Excelente cifrado.
- 👍 No es bloqueado por los ISPs*.
- 😬 Requiere certificados digitales (propios o comprados).

Configuración específica para SSTP

1. Habilitarlo.
2. Configurar la autenticación a sólo mschap2.
3. Seleccionar el certificado del servidor*.

```
/interface sstp-server server set \  
enabled=yes \  
authentication=mschap2 \  
certificate=cert_vpn
```



Configuración específica para SSTP

Ejemplo con
cliente Windows 10

The image shows a Windows 10 configuration window titled "Configuración" with a sub-header "VPN". The main content area is blue and titled "Agregar una conexión VPN". It contains several fields and dropdown menus:

- Proveedor de VPN:** A dropdown menu set to "Windows (integrado)".
- Nombre de conexión:** A text input field containing "VPN SSTP".
- Nombre de servidor o dirección:** A text input field containing "vpn.dominio.com", highlighted with a red box.
- Tipo de VPN:** A dropdown menu set to "Protocolo de túnel de sockets seguros (SSTP)", highlighted with a red box.
- Tipo de información de inicio de sesión:** A dropdown menu set to "Nombre de usuario y contraseña".
- Nombre de usuario (opcional):** A text input field containing "usuario", highlighted with a red box.
- Contraseña (opcional):** A text input field with masked characters (dots), highlighted with a red box.
- Recordar información de inicio de sesión:** A checked checkbox.

At the bottom right, there are two buttons: "Guardar" and "Cancelar".

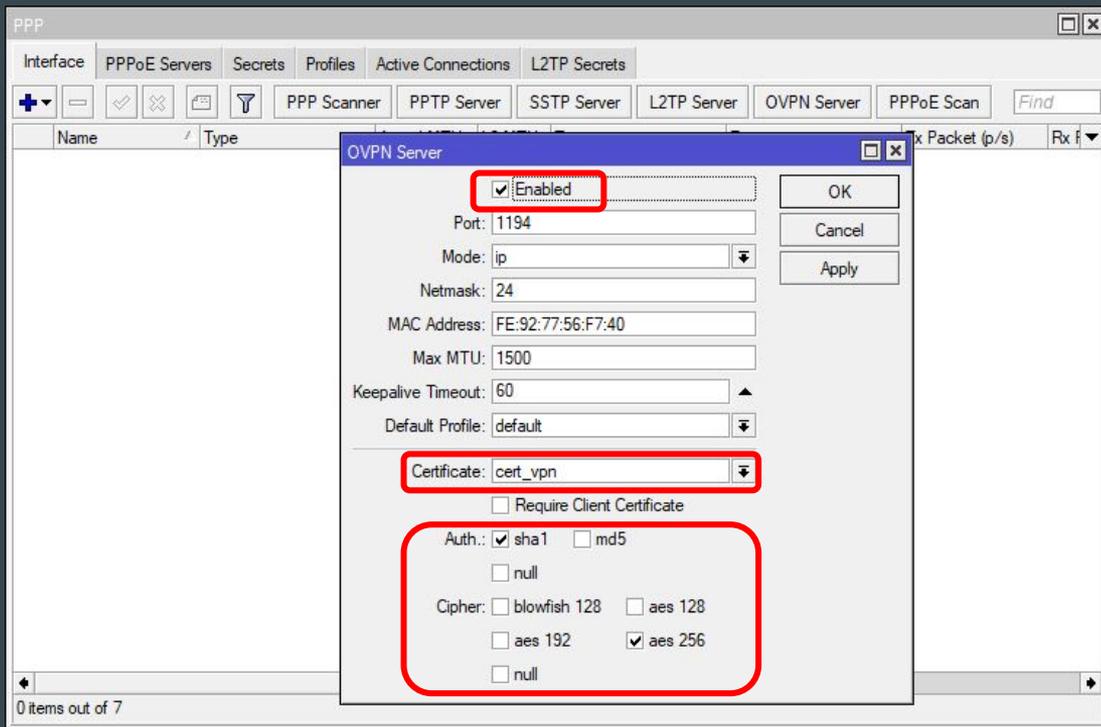
Configuración específica para OpenVPN

- OpenVPN utiliza **TCP / UDP 1194** para levantar un túnel entre cliente y servidor. En UDP funciona “mejor”, aunque de momento sólo está disponible en RouterOS v7.
 - 👍 Excelente compatibilidad (hay que descargar el cliente OVPN)
 - 👍 Excelente cifrado.
 - 👍 No es bloqueado por los ISPs*.
 - 😬 Requiere certificados digitales (propios o comprados).
 - 💖 Se puede distribuir configuración a los clientes mediante un script .ovpn.

Configuración específica para OpenVPN

1. Habilitarlo.
2. Configurar la autenticación con SHA1 y cifrado AES256.
3. Seleccionar el certificado del servidor*.

```
/interface ovpn-server server set \  
enabled=yes \  
auth=sha1 cipher=aes256 \  
certificate=cert_vpn
```



Configuración específica para OpenVPN

Estructura de archivo de configuración.

```
client
dev tun
remote vpn.dominio.com 1194 tcp-client
auth-user-pass
cipher AES-256-CBC
<ca>
# INSERTAR CERTIFICADO DEL SERVIDOR AQUÍ #
</ca>
route 10.20.30.0 255.255.255.0 vpn_gateway
```

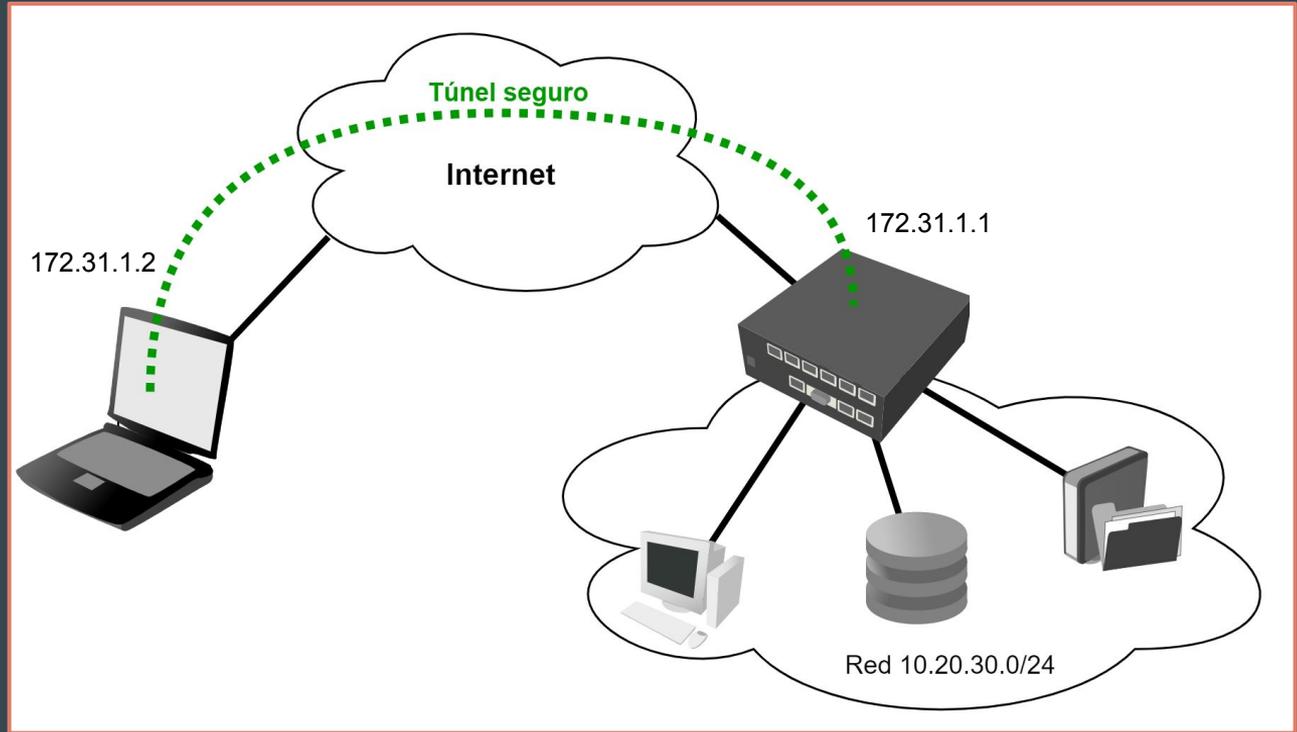


Se puede definir rutas específicas!

Configuración específica

Escenario final:

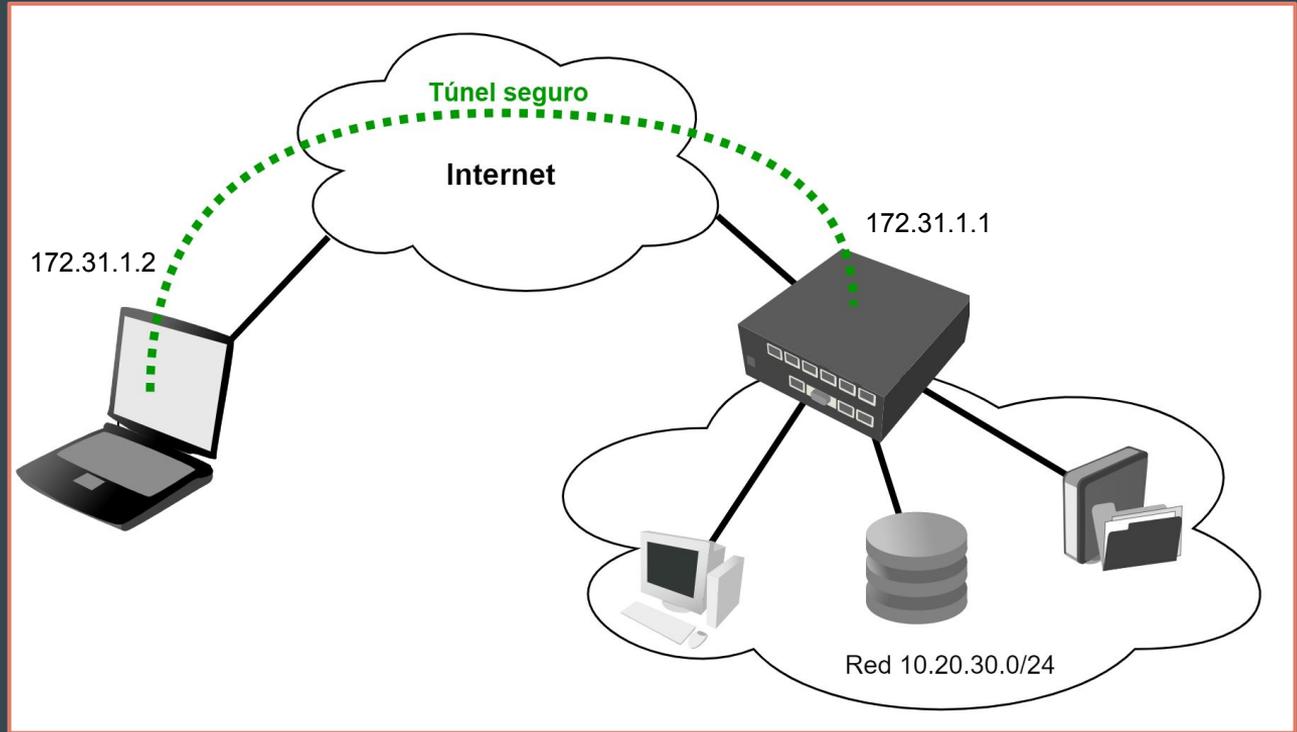
- Mikrotik con IP pública
- Red LAN 10.20.30.0/24
- Cliente remoto con IP pública o privada.
- Luego de crear el cliente en la PC, podemos acceder a la red remota a través de un túnel seguro!



Routing sobre VPNs

Escenario final:

- En este escenario, tenemos acceso a la red remota.
- Pero todo el tráfico, incluida la navegación por Internet, sale por la red remota, ya que así viene por defecto la configuración en los clientes L2TP+IPSec y en SSTP.
- **En OVPN podemos cargar las rutas en el archivo de configuración.**



BONUS: Creación de certificados autofirmados

```
# Crear certificado raíz o CA (Certification Authority o Autoridad Certificadora).  
/certificate add name=cert_ca common-name=ca.dominio.com days-valid=365
```

```
# Autofirmar certificado  
/certificate sign cert_ca
```

```
# Crear certificado para el servidor VPN  
/certificate add name=cert_vpn common-name=vpn.dominio.com days-valid=365
```

```
# Firmar certificado con el CA previamente creado  
/certificate sign cert_vpn ca=cert_ca
```

```
# Exporta certificado (aparece en Files, luego de descargarlo se puede borrar el archivo)  
/certificate export-certificate cert_vpn
```



TIP: es crucial que *common-name* sea el nombre de dominio o IP pública del servidor VPN.

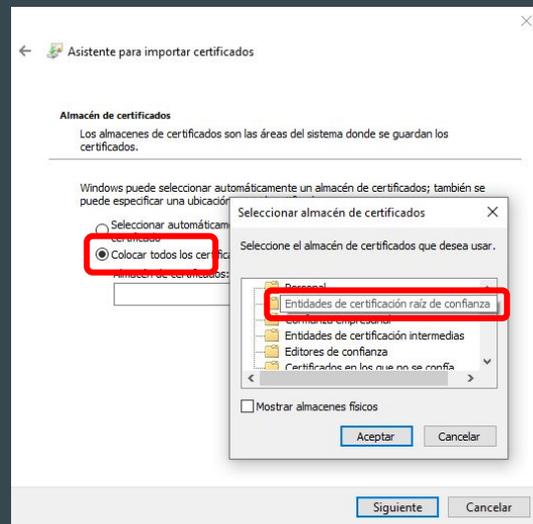
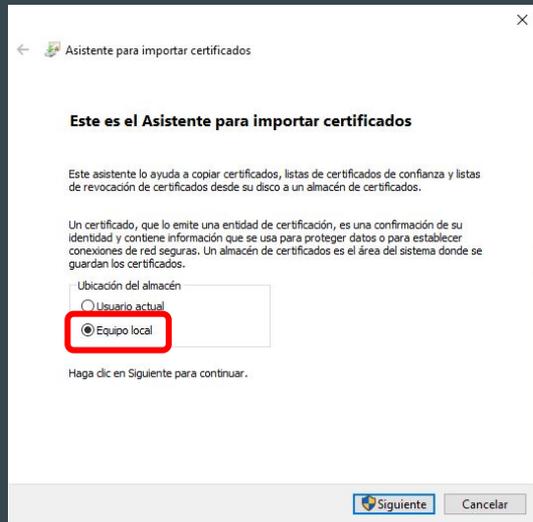
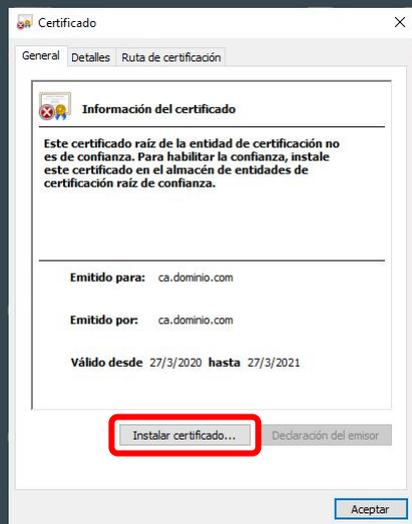
BONUS: Creación de certificados autofirmados

`cert_vpn.crt` es el certificado exportado y se vería así:

```
-----BEGIN CERTIFICATE-----
MIIDHCCAgSgAwIBAgIIe15Xx8mw588wDQYJKoZIhvcNAQELBQAwGTEXMBUGA1UE
AwwOY2EuZG9taW5pby5jb20wHhcNMjAwMzI3MDMzMzUwWhcNMjAwMzI3MDMzMzUw
WjAAMRcwFQYDVQQLDAA5jYS5kb21pbmlvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALuaCZMgMwOfHCj5RG+D5XOp43doh6J8LR1tRJKUhQbjXyes
G93g8enWoiRzk7B3J6qy9XJvi2Ve5EMIEnhBoQHKRYJRWOu0boNMVp7EOYtLhAJH
crMEB+uln7EGJz5TY22hNs6tiOMyfCEiIMeCWY/o/b3KQNAo/v+r4P5CCcQQtIFF
pgq6bHVIDz/m70fQWemb8w9pMs4JtqxOfckDHL1MSPXiDcXP8JOBxt12/3/PP1ap
DNgnV3F/XNLmxP4LVxFVU8zVb/lANiWXo6mXmtQce5dLZfDXKlJ/kclFKucIJGTf
Uuj9sarSft6ccUuQL2vrwh84QVgW5cMHnI7uOQsCAwEAAaNoMGYwDwYDVR0TAQH/
BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAbYwHQYDVR0OBBYEFMwIOir1ILg3GSETxHGV
UOg58RdYMCQGCGSAGG+EIBDQXFFhVHZW5lcmF0ZWQgYnkgUm91dGVyT1MwDQYJ
KoZIhvcNAQELBQADggEBAH++NRJg1KPU71Kt5JJ9/xPmFzsVj1Qf6PQO67LcHN+Y
ALRqyp43dbcWhZEmnLHDtKsLvW+TS1tV/fl36T5EtTAkfpniS+r3jrqcBwp5Zbwx
2QHmChtpzbGf+PRX8yWnJkQy+IMvWQIBXSMOQ1iGOSG7qOQL12k0YsJYOAEzVTLb
+hLaseoQBM4qZxs2O7TXNXdjucdIYuR4ZWQ8xjMeJP/uNR5apJT+uGLcrmsbEDBG
NOWw49T5im/IIt3ViLzxxOBDyWhiTDV3l/qHqVvNTXOcF574kzWRdNXHfvOU1o+l
mhiJTsq4gQzwvoSaG+byGF858s81dMCev32x2WTBpTM=
-----END CERTIFICATE-----
```

BONUS: Creación de certificados autofirmados

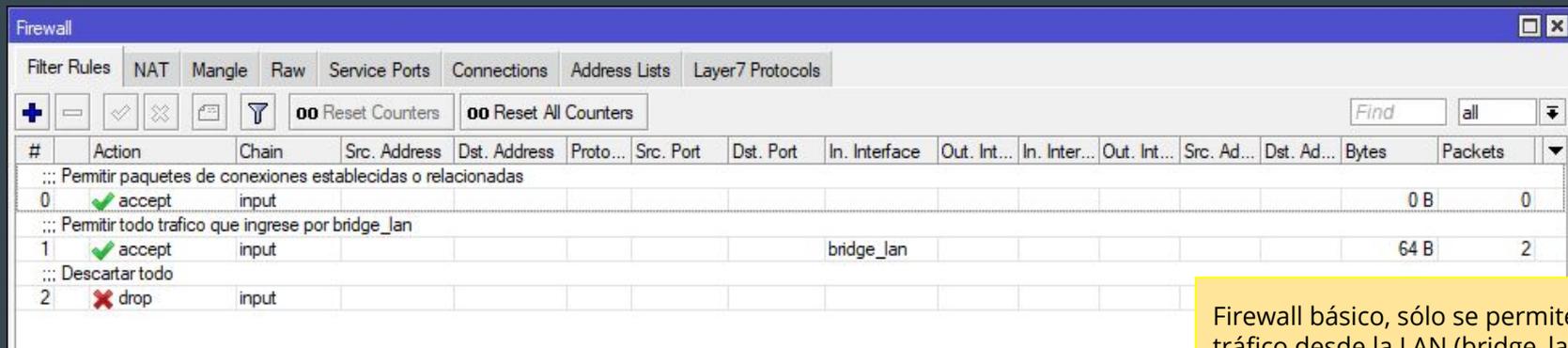
Instalación de certificado raíz en Windows 10:



Aspectos de seguridad en el Firewall de RouterOS

Aspectos de seguridad en el Firewall de RouterOS

- Una falla común en estas implementaciones es no dejar los puertos abiertos correctamente, entonces los clientes no pueden conectarse!
- Se hará un repaso de los requerimientos de cada protocolo y exponer un firewall sencillo que permita el acceso por VPN (sea cual fuera el protocolo elegido).



The screenshot shows the RouterOS Firewall configuration interface. The 'Filter Rules' tab is active. The configuration table is as follows:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	accept	input												0 B	0
1	accept	input						bridge_lan						64 B	2
2	drop	input													

Firewall básico, sólo se permite tráfico desde la LAN (bridge_lan).

Aspectos de seguridad en el Firewall de RouterOS

- L2TP+IPSec
 - UDP 1701, UDP 500, UDP 4500
 - Protocolo IPSec-ESP
- SSTP
 - Protocolo TCP 443*
- OpenVPN
 - Protocolo TCP 1194* o UDP 1194* (sólo ROSv7)

Aspectos de seguridad en el Firewall de RouterOS

#	Action	Chain	Src. Address	Dst. A...	Protocol	Src. Port	Dst. Port	In. Interface	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
::: Permitir paquetes de conexiones establecidas o relacionadas															
0	✓ accept	input												176.7 KiB	738
::: Permitir todo trafico que ingrese por bridge_lan															
1	✓ accept	input						bridge_lan						208 B	4
::: Permitir acceso L2TP															
2	✓ accept	input			17 (udp)		1701,500,4500							125 B	1
::: Permitir acceso IPSec															
3	✓ accept	input			50 (ipsec-esp)									336 B	2
::: Permitir acceso SSTP															
4	✓ accept	input			6 (tcp)		443							52 B	1
::: Permitir acceso OpenVPN															
5	✓ accept	input			6 (tcp)		1194							208 B	4
::: Descartar todo															
6	✗ drop	input												12.0 KiB	137

7 items

Aspectos de seguridad en el Firewall de RouterOS

```
/ip firewall filter
```

```
add comment="Permitir paquetes de conexiones establecidas o relacionadas" \  
chain=input connection-state=established,related action=accept
```

```
add comment="Permitir todo trafico que ingrese por bridge_lan" chain=input \  
in-interface=bridge_lan action=accept
```

```
add comment="Permitir acceso L2TP" protocol=udp dst-port=1701,500,4500 action=accept
```

```
add comment="Permitir acceso IPSec" chain=input protocol=ipsec-esp action=accept
```

```
add comment="Permitir acceso SSTP" chain=input protocol=tcp dst-port=443 action=accept
```

```
add comment="Permitir acceso OpenVPN" chain=input protocol=tcp dst-port=1194 action=accept
```

```
add comment="Descartar todo" chain=input action=drop
```



prozcenter



prozcenter



prozcenter



VPNs seguras con Mikrotik RouterOS